UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. **Case No. 16-CR-103**

NEIL C. KIENAST,

Defendant.

RECOMMENDATION ON DEFENDANT'S MOTION TO SUPPRESS

Neil C. Kienast is charged with possessing child pornography. The charge stems from the FBI's investigation of "Website A," a site alleged to be dedicated to the advertisement and distribution of child pornography. The FBI seized control of Website A and obtained from a magistrate judge in the Eastern District of Virginia a search warrant that allowed the government to use a "Network Investigative Technique" (NIT) to identify individual users who were accessing content on the site. Upon deploying the NIT and conducting additional investigation, the FBI identified Mr. Kienast as a user of Website A. Law enforcement officers used this information to secure a warrant to search Mr. Kienast's home. Upon executing the warrant, officers recovered several computers and storage media that contained numerous images and videos of suspected child pornography. Mr. Kienast also admitted to officers that he had been viewing child pornography for the past several years.

On August 10, 2016, Mr. Kienast filed a motion to suppress the fruits of the residence search. He contends that the warrant to search his residence is invalid because it was obtained using information gathered from two unlawful searches: the search pursuant to the NIT Warrant and the release of his personal identifying information at the Social Security Administration. The United States argues that the NIT Warrant is valid and that suppression would nevertheless be an inappropriate remedy in this case. The United States also argues that Mr. Kienast does not have a reasonable expectation of privacy in his identifying information. For the following reasons, the Court will recommend that Mr. Kienast's motion be denied.

I. Background

In September 2014, FBI agents began investigating a website that appeared to be dedicated to the advertisement and distribution of child pornography. Affidavit in Support of Application for NIT Warrant ¶ 11, ECF No. 12-3 at 6-38. The website—referred to in the warrant applications as Target Website and Website A, respectively—operated on the anonymous Tor network, which allowed users to mask their Internet Protocol addresses while accessing the site, NIT Aff. ¶¶ 7-8. In February 2015, the FBI apprehended the website's administrator and assumed administrative control of the site. NIT Aff. ¶ 30. The FBI allowed the site to continue to operate from a computer server that was located at a government facility within the Eastern District of Virginia.

On February 20, 2015, an FBI special agent applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use a Network Investigative Technique to investigate the users and administrators of Website A. In support of the warrant application, the agent submitted a thirty-three-page affidavit that set forth his basis for probable cause to believe that deploying the NIT would uncover evidence and instrumentalities of certain child exploitation crimes. *See generally* NIT Aff. The affidavit described in detail the FBI's investigation of Website A, including the site's nature and content and how users could find and access it. NIT Aff. ¶¶ 6-27 The affidavit also described how the NIT worked and why it was believed to be a necessary step in the investigation. NIT Aff. ¶¶ 28-37.

The NIT involved additional computer instructions that would be downloaded to a user's computer—referred to as an activating computer—along with the site's normal content. NIT Aff. ¶ 33. After downloading the additional instructions, the activating computer would transmit certain information to the government-controlled computer located in the Eastern District of Virginia, including: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" address. NIT Aff. ¶¶ 33-34, 36. The NIT would be deployed each time a user logged onto the government-controlled website. NIT Aff. ¶ 36.

United States Magistrate Judge Theresa Carroll Buchanan, sitting in the Eastern District of Virginia, signed the NIT Warrant on February 20, 2015. NIT Search Warrant, ECF No. 12-3 at 3-5. Agents executed the warrant that same day and continued to collect data from computers that accessed Website A until March 4, 2015. NIT Search Warrant Return, ECF No. 12-3 at 39-40.

Through the use of the NIT and additional investigation, FBI agents determined that an individual with the username "Playpendrifter" registered an account on Website A on December 9, 2014, and accessed the site for more than ten hours between December 9 and March 4, 2015. Affidavit in Support of Application for Warrant to Search Mr. Kienast's Residence ¶¶ 27-28, ECF No. 12-1 at 2-32. This user accessed several posts that contained links to and sample photos of child pornography. Residence Aff. ¶¶ 30-33. Agents learned the user's IP address, host name, and logon name via the NIT; determined the service provider of the IP address; and linked the IP address to Mr. Kienast at the home he shared with his parents in Oshkosh, Wisconsin. Residence Aff. ¶ 29-30, 34-41. Agents also learned Mr. Kienast's personal identifying information from a "confidential source" at the Social Security Administration. Defendant's Motion for Suppression of Evidence Due to Invalid Warrants ¶ 10, ECF No. 10.

An FBI agent subsequently applied for a warrant to search the Oshkosh residence. In support of the warrant application, the agent submitted a thirty-one-page affidavit that set forth his basis for probable cause to believe that the residence contained evidence relating to federal violations concerning child

pornography. *See generally* Residence Aff. This affidavit recited much of the information contained in the NIT Warrant affidavit. *See* Residence Aff. ¶¶ 7-22. United States Magistrate Judge James R. Sickel signed the warrant on January 12, 2016. Warrant to Search Mr. Kienast's Residence, ECF No. 12-2.

Law enforcement officers executed the warrant on January 14, 2016, and seized several computers and storage media located in the residence. Government's Response to Defendant[']s Motion to Suppress Evidence and Statements 1, ECF No. 12. A subsequent search of the computers revealed images and videos containing child pornography. *Id.* at 1-2. Upon being interviewed by law enforcement officers, Mr. Kienast admitted to viewing child pornography for the past several years and acknowledged using the Tor network to do so. *Id.* at 2.

Based on the evidence seized from the residence and his statement to law enforcement, Mr. Kienast was charged on June 28, 2016, with one count of knowingly possessing matter that contained images of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Indictment, ECF No. 1-1. The matter is assigned to United States District Judge William C. Griesbach for trial and to this Court for pretrial motions. Mr. Kienast's trial is currently scheduled for September 19, 2016.

II. Discussion

In support of his motion to suppress, Mr. Kienast argues that the issuing magistrate judge lacked jurisdiction to authorize the NIT Warrant under the Federal Magistrates Act, 28 U.S.C. § 636(a), and that the warrant does not comply

with the territorial restrictions of Rule 41(b) of the Federal Rules of Criminal Procedure. He relies principally upon *United States v. Levin*, Criminal Action No. 15-10271-WGY, 2016 U.S. Dist. LEXIS 52907 (D. Mass. Apr. 20, 2016), a recent district court decision involving the same NIT Warrant at issue here. Mr. Kienast further maintains that investigators failed to secure a warrant to obtain his identifying information from the SSA.[1]

The United States argues that the NIT Warrant complied with the provisions of Rule 41 and that, in any event, suppression is not a proper remedy here. The United States also contends that the issuing magistrate judge had inherent power to authorize the NIT Warrant and that the FBI relied on the warrant in good faith.

A. Relevant law

"Section 636(a) of the Federal Magistrates Act establishes 'jurisdictional limitations on the power of magistrate judges[.]'" Def.'s Mot. ¶ 4 (quoting *United*

[1] In his reply brief, Mr. Kienast argues that the NIT Warrant is also invalid because the use of the NIT source code was an unconstitutional search, the warrant is overbroad, and the warrant lacks specificity regarding the area to be searched or how the search was to be conducted. Defendant[']s Reply To Government[']s Response to Defendant[']s Motion to Suppress Evidence and Statements 3-5, 10, ECF No. 14. These arguments are waived, as they were made for the first time in reply. *See United States v. Diaz*, 533 F.3d 574, 577 (7th Cir. 2008) ("Arguments may not be raised for the first time in a reply brief."). Moreover, numerous courts have rejected similar arguments, *see, e.g.*, *United States v. Matish*, Criminal No. 4:16cr16, 2016 U.S. Dist. LEXIS 82279 (E.D. Va. June 23, 2016), and Mr. Kienast offers no compelling reason to chart a different course here.

Mr. Kienast also makes passing reference in his reply brief to the NIT source code. Def.'s Reply 3-4, 6, 10-11. To the extent he seeks an order compelling the United States to reveal the source code, this request is denied as untimely and immaterial to resolving his suppression motion.

States v. Krueger, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring)). It provides, in relevant part, as follows:

> (a) Each United States magistrate judge serving under this chapter shall have *within the district in which sessions are held* by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> > (1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure for the United States District Courts.

28 U.S.C. § 636(a) (emphasis added).

"Rule 41(b) sets out five alternative territorial limits on a magistrate judge's authority to issue a warrant." *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013). Specifically, Rule 41(b) authorizes magistrate judges to issue warrants to (1) "search for and seize a person or property located within [the judge's] district"; (2) search for and seize a person or property located outside the judge's district "if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (3) search for and seize a person or property located outside the judge's district if the investigation relates to terrorism; (4) "install within [the judge's] district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both; or (5) search for and seize a person or property located outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomatic or consular mission. *See* Fed. R. Crim. P. 41(b).

In *United States v. Levin*, 2016 U.S. Dist. LEXIS 52907, at *46, the district court granted a motion to suppress that raised the same issues Mr. Kienast raises here, finding the NIT Warrant void ab initio. The court first held that the issuing magistrate judge lacked authority to issue the NIT Warrant under § 636(a) or any of the five provisions of Rule 41(b). *Levin*, 2016 U.S. Dist. LEXIS 52907, at *9-18. The court then determined that suppression was an appropriate remedy because the magistrate judge lacked jurisdiction to issue the NIT Warrant and because the defendant suffered prejudice as a result. *Id.* at *18-29. The court also concluded that the good-faith exception does not apply to warrants void at the outset due to lack of jurisdiction. *Id.* at *29-42. Lastly, the court explained that its decision did not create "an insurmountable legal barrier" to law enforcement efforts concerning such investigations, as the government could have obtained the NIT Warrant from a district judge (because the territorial limits in § 636(a) and Rule 41(b) apply only to magistrate, not district, judges) or could seek amendment of Rule 41(b) to account for this issue. *Id.* at *42-46.

B. Analysis

Mr. Kienast argues that the NIT Warrant authorized a search of property located outside the issuing magistrate judge's district because the warrant permitted the FBI to search the personal computers of users of Website A no matter where those computers were located. Def.'s Mot. 3-4; Def.'s Reply 1-4, 10. As such, he contends that the issuing judge exceeded the territorial bounds provided in § 636(a) and Rule 41(b) and, therefore, lacked authority to issue the NIT Warrant.

The United States argues that Rule 41(b) should be read broadly to allow for the issuance of warrants to investigate Tor hidden services. Govt.'s Resp. 9-11. Specifically, the United States contends that the Eastern District of Virginia magistrate judge had authority to issue the NIT Warrant under subsections (1), (2), or (4) of Rule 41(b). The United States further maintains that the NIT Warrant was issued consistent with the Fourth Amendment and "by a judge with the strongest known connection to the [proposed] search." *Id.* at 11-12.

Although Mr. Kienast raises an interesting and compelling issue—indeed, a number of courts around the country have rendered decisions concerning the same investigation at issue here, *see, e.g.*, *United States v. Henderson*, Case No. 15-cr-00565-WHO-1, 2016 U.S. Dist. LEXIS 118608 (N.D. Cal. Sept. 1, 2016)—to resolve his suppression motion, the Court need not determine whether the magistrate judge lacked authority to issue the NIT Warrant under § 636(a) or Rule 41(b). That is, assuming that the magistrate judge lacked jurisdiction to issue the NIT Warrant, the Court nevertheless concludes, based on Seventh Circuit case law, that suppression would not be an appropriate remedy in this case.

In *United States v. Berkos*, 543 F.3d 392, 395 (7th Cir. 2008), a magistrate judge issued a warrant compelling an out-of-district internet service provider to disclose electronic communications records relating to an ongoing criminal investigation. The defendant maintained on appeal that the district court erred in denying his motion to suppress, asserting that the magistrate judge had exceeded the jurisdictional limitations of Rule 41(b) in authorizing the warrant. *Id.* at 396.

The Seventh Circuit indicated that the defendant's argument required the court to determine whether a violation of Rule 41(b) merits invoking the exclusionary rule. *Id.*

In addressing this issue, the court first noted that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval." *Id.* (quoting *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008)); *see also United States v. Trost*, 152 F.3d 715, 722 (7th Cir. 1998). The court further noted that "[t]he remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the wrong.'" *Berkos*, 543 F.3d at 396 (quoting *Cazares-Olivas*, 515 F.3d at 730). "This alone," according to the court, would merit "affirming the district court's denial of [the defendant's] . . . motion to suppress." *Berkos*, 543 F.3d at 396. Because the United States had failed to make such an argument, however, the court went on to address the merits of the defendant's appeal.

In light of *Berkos*, the Court finds that the evidence at issue here should not be suppressed because it was obtained via a judicially authorized warrant supported by probable cause. *See, e.g.*, *United States v. Epich*, Case No. 15-CR-163-PP, 2016 U.S. Dist. LEXIS 32459 (E.D. Wis. Mar. 14, 2016). Mr. Kienast does not argue otherwise. Suppression would be particularly inappropriate in this case given that there is no evidence that the FBI deliberately sought the NIT Warrant from a judge who lacked authority to issue it. To the extent the NIT Warrant is invalid for

lack of jurisdiction, that error was made by the issuing judge. The purpose of the exclusionary rule, however, is "to deter illegal police conduct, not mistakes by judges and magistrates." *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986). The only mistake law enforcement made here was knocking on the wrong door in seeking authorization for the NIT Warrant. *See Levin*, 2016 U.S. Dist. LEXIS 52907, at *43-46 (finding that the NIT Warrant could have been issued by one of the seven Article III judges who routinely sit in the Alexandria Courthouse within the Eastern District of Virginia).

For these same reasons, Mr. Kienast cannot show that he was prejudiced in any way by having a magistrate judge (rather than a district judge) issue the NIT Warrant. There is nothing in the record suggesting that the magistrate judge failed to exercise neutral and detached judgment, and the absence of an attack on whether probable cause existed tends to confirm the correctness of that judgment. At bottom, the exclusionary rule exists to preserve the guarantees of the Fourth Amendment, and the government acted in accord with those guarantees in this case. Suppression under these circumstances would improperly elevate form over substance.

C. Conclusion

Here, Mr. Kienast seeks to suppress the fruits of the residence search, arguing that the Residence Warrant was unlawfully obtained using information gathered from the search pursuant to the NIT Warrant and the release of his personal identifying information at the SSA. The Court concludes, however, that the NIT Warrant satisfied the requirements of the Fourth Amendment and that

suppression would be "wildly out of proportion" to any purported lack of authority in issuing it. Likewise, the Residence Warrant did not include any information gathered from the SSA, *see* Residence Aff. ¶¶ 34-41, and, in any event, Mr. Kienast lacks a reasonable expectation of privacy in this information, *see United States v. Miller*, 425 U.S. 435, 439-45 (1976) (finding no reasonable expectation of privacy in personal records held by third parties). Accordingly, the Court will recommend that the district judge deny Mr. Kienast's motion to suppress.

NOW, THEREFORE, IT IS HEREBY RECOMMENDED that Mr. Kienast's Motion for Suppression of Evidence Due To Invalid Warrants, ECF No. 10, be **DENIED**.

Your attention is directed to 28 U.S.C. § 636(b)(1)(B) and (C), Fed. R. Crim. P. 59(b), and E.D. Wis. Gen. L. R. 72(c), whereby written objections to any recommendation herein, or part thereof, may be filed within fourteen days of service of this Recommendation or prior to the Jury Trial date, whichever is earlier. Objections are to be filed in accordance with the Eastern District of Wisconsin's electronic case filing procedures. Failure to file a timely objection with the district court shall result in a waiver of a party's right to appeal. If no response or reply will be filed, please notify the Court in writing.

Dated at Milwaukee, Wisconsin, this 7th day of September, 2016.

BY THE COURT:

s/ David E. Jones
DAVID E. JONES
United States Magistrate Judge